

## UNITED STATES DISTRICT COURT

for the  
Southern District of OhioIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)Google, LLC records and accounts that record location  
information for devices as detailed in Attachments A and  
B

Case No. 2:22-mj-713

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under  
penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the  
property to be searched and give its location):

See Attachment A

located in the Northern District of California, there is now concealed (identify the  
person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):


- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC 1951	Interference with Interstate Commerce through Robbery
18 USC 924(c)(1)(A)(ii)	Brandishing a Firearm During a Crime of Violence

The application is based on these facts:

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested  
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Brian V. Boesch, ATF Task Force Officer

Printed name and title

Sworn to before me and signed in my presence.

Date: October 28, 2022

City and state: Columbus, OH


  
Kimberly A. Johnson  
United States Magistrate Judge


IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF  
LOCATION INFORMATION FOR  
RECORDS AND ACCOUNTS THAT ARE  
STORED AT PREMISES CONTROLLED  
BY GOOGLE

**FILED UNDER SEAL**

Case No. 2:22-mj-713

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Task Force Officer (TFO) Brian V. Boesch, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a warrant to search information that is stored at premises controlled by Google, an electronic communication service and remote computing service provider headquartered in Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a warrant under 18 U.S.C. § 2703(c)(1)(A) to require Google to disclose to the government the information further described in Attachment B.I. The government will then review that information and seize the information that is further described in Attachment B.II.

2. I am a Task Force Officer with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), and I have been since July 6, 2014. Prior to being selected as a TFO, I began service with the Columbus Division of Police on November 6, 1994. In February 2006, I began working as a robbery detective with CPD, a position I held for 8 ½ years. Through training and experience, I have come to learn that Google maintains location data for devices that use their

applications and stores that data under specific device IDs. Biographical information associated with those device IDs can later be obtained from Google.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1951 and 18 U.S.C. § 924(c) have been committed and are being committed by unknown persons. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

### **JURISDICTION**

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### **BACKGROUND RELATING TO GOOGLE AND RELEVANT TECHNOLOGY**

6. Based on my training and experience, I know that cellular devices, such as mobile telephone(s), are wireless devices that enable their users to send or receive wire and/or electronic communications using the networks provided by cellular service providers. Using cellular networks, users of many cellular devices can send and receive communications over the Internet.

7. I also know that many devices, including but not limited to cellular devices, have the ability to connect to wireless Internet (“wi-fi”) access points if the user enables wi-fi connectivity. These devices can, in such cases, enable their users to send or receive wire and/or electronic communications via the wi-fi network. A tablet such as an iPad is an example of a

device that may not have cellular service but that could connect to the Internet via wi-fi. Wi-fi access points, such as those created through the use of a router and offered in places like homes, hotels, airports, and coffee shops, are identified by a service set identifier (“SSID”) that functions as the name of the wi-fi network. In general, devices with wi-fi capability routinely scan their environment to determine what wi-fi access points are within range and will display the names of networks within range under the device’s wi-fi settings.

8. Based on my training and experience, I also know that many devices, including many cellular and mobile devices, feature Bluetooth functionality. Bluetooth allows for short-range wireless connections between devices, such as between a device such as a cellular phone or tablet and Bluetooth-enabled headphones. Bluetooth uses radio waves to allow the devices to exchange information. When Bluetooth is enabled, a device routinely scans its environment to identify Bluetooth devices, which emit beacons that can be detected by devices within the Bluetooth device’s transmission range, to which it might connect.

9. Based on my training and experience, I also know that many cellular devices, such as mobile telephones, include global positioning system (“GPS”) technology. Using this technology, the device can determine its precise geographical coordinates. If permitted by the user, this information is often used by apps installed on a device as part of the apps’ operation.

10. Based on my training and experience, I know Google is a company that, among other things, offers an operating system (“OS”) for mobile devices, including cellular phones, known as Android. Nearly every device using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.

11. In addition, based on my training and experience, I know that Google offers numerous apps and online-based services, including messaging and calling (*e.g.*, Gmail, Hangouts, Duo, Voice), navigation (Maps), search engine (Google Search), and file creation, storage, and sharing (*e.g.*, Drive, Keep, Photos, and YouTube). Many of these services are accessible only to users who have signed in to their Google accounts. An individual can obtain a Google account by registering with Google, and the account identifier typically is in the form of a Gmail address (*e.g.*, example@gmail.com). Other services, such as Maps and YouTube, can be used with limited functionality without the user being signed in to a Google account.

12. Based on my training and experience, I also know Google offers an Internet browser known as Chrome that can be used on both computers and mobile devices. A user has the ability to sign-in to a Google account while using Chrome, which allows the user's bookmarks, browsing history, and other settings to be uploaded to Google and then synced across the various devices on which the subscriber may use the Chrome browsing software, although Chrome can also be used without signing into a Google account. Chrome is not limited to mobile devices running the Android operating system and can also be installed and used on Apple devices and Windows computers, among others.

13. Based on my training and experience, I know that, in the context of mobile devices, Google's cloud-based services can be accessed either via the device's Internet browser or via apps offered by Google that have been downloaded onto the device. Google apps exist for, and can be downloaded to, devices that do not run the Android operating system, such as Apple devices.

14. According to my training and experience, as well as open-source materials published by Google, I know that Google offers accountholders a service called "Location

History,” which authorizes Google, when certain prerequisites are satisfied, to collect and retain a record of the locations where Google calculated a device to be based on information transmitted to Google by the device. That Location History is stored on Google servers, and it is associated with the Google account that is associated with the device. Each account holder may view their Location History and may delete all or part of it at any time.

15. Based on my training and experience, I know that the location information collected by Google and stored within an account’s Location History is derived from sources including GPS data and information about the wi-fi access points and Bluetooth beacons within range of the device. Google uses this information to calculate the device’s estimated latitude and longitude, which varies in its accuracy depending on the source of the data. Google records the margin of error for its calculation as to the location of a device as a meter radius, referred to by Google as a “maps display radius,” for each latitude and longitude point.

16. Based on open-source materials published by Google and my training and experience, I know that Location History is not turned on by default. A Google account holder must opt-in to Location History and must enable location reporting with respect to each specific device and application on which they use their Google account in order for that usage to be recorded in Location History. A Google account holder can also prevent additional Location History records from being created at any time by turning off the Location History setting for their Google account or by disabling location reporting for a particular device or Google application. When Location History is enabled, however, Google collects and retains location data for each device with Location Services enabled, associates it with the relevant Google account, and then uses this information for various purposes, including to tailor search results based on the user’s location, to determine the user’s location when Google Maps is used, and to

provide location-based advertising. As noted above, the Google accountholder also has the ability to view and, if desired, delete some or all Location History entries at any time by logging into their Google account or by enabling auto-deletion of their Location History records older than a set number of months.

17. Location data, such as the location data in the possession of Google in the form of its users' Location Histories, can assist in a criminal investigation in various ways. As relevant here, I know based on my training and experience that Google has the ability to determine, based on location data collected and retained via the use of Google products as described above, devices that were likely in a particular geographic area during a particular time frame and to determine which Google account(s) those devices are associated with. Among other things, this information can indicate that a Google accountholder was near a given location at a time relevant to the criminal investigation by showing that his/her device reported being there.

18. Based on my training and experience, I know that when individuals register with Google for an account, Google asks subscribers to provide certain personal identifying information. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, this information often provide clues to their identity, location, or illicit activities.

19. Based on my training and experience, I also know that Google typically retains and can provide certain transactional information about the creation and use of each account on



its system. This information can include the date on which the account was created, the length of service, records of login (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, Google often has records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

### **PROBABLE CAUSE**

20. On October 5, 2022, at 12:15am, a male white entered the Shell Gas Station located at 5340 Tuttle Crossing Blvd., Dublin, Ohio, within the Southern District of Ohio. As the suspect approached the clerk, the suspect lifted his shirt to reveal a handgun in his waistband and said, "Do it!" The suspect ordered the clerk to open both registers and put the cash into a store bag. The clerk complied and the suspect fled the store. The suspect was wearing a black balaclava that covered his face, a black sweatshirt, and black sweatpants. He was wearing orange or red flip flops or slides with no socks.

21. On October 10, 2022, at 1:43am, a male white entered the Speedway located at 1434 Bethel Rd., Columbus, Ohio, within the Southern District of Ohio, after parking his lime green Kia Soul in front of the store. The male approached the clerk and lifted his shirt to reveal a handgun tucked in his waistband. The clerk handed the suspect the cash and he fled northbound on Godown Rd. in the green Kia. The suspect was wearing a black balaclava, black sweatshirt, and black shorts. He was also wearing the same slides as the suspect from the Shell robbery.



22. On October 22, 2022, at 11:17pm, a male white entered Marco's Pizza located at 4996 Cosgray Rd., Dublin, Ohio, within the Southern District of Ohio. The suspect approached the clerks and demanded money from the register. When the female clerk asked if he was serious, the suspect lifted his shirt to reveal a handgun in his waistband. The clerk handed the suspect approximately \$75 in cash and the suspect fled in a green Kia Soul that was parked near the front of the store. The suspect was wearing a black balaclava, black sweatshirt, khaki shorts and orange slides.

23. Prior to entering Marco's Pizza, the unknown suspect parked his car near the front door of the restaurant and remained inside the car for several moments before entering the store, allowing for the possibility that the suspect was on his cellular phone. In addition, the three (3) robbery locations are separated by several miles and are serviced by multiple different cellular towers. Therefore, the possibility that multiple cell phones accessing the specific cell tower at the exact date and time of the three (3) robberies is slim. In my sixteen (16) years investigating robberies, it is common for suspects to have their cell phones on or near them at the time of their offenses.

24. Based on the foregoing, I submit that there is probable cause to search information that is currently in the possession of Google and that relates to the devices that reported being within the Target Locations described in Attachment A during the time period described in Attachment A for evidence of the crime(s) under investigation. The information to be searched includes (1) identifiers of each device; (2) the location(s) reported by each device to Google and the associated timestamp; and (3) basic subscriber information for the Google account(s) associated with each device.

25. The proposed warrant sets forth a multi-step process whereby the government will obtain the information described above. Specifically, as described in Attachment B.I:

- a. Using Location History data, Google will identify those devices that it calculated were or could have been (based on the associated margin of error for the estimated latitude/longitude point) within the Target Locations described in Attachment A during the time period described in Attachment A. For each device, Google will provide a anonymized identifier, known as a Reverse Location Obfuscation Identifier (“RLOI”), that Google creates and assigns to devices for purposes of responding to this search warrant; Google will also provide each device’s location coordinates along with the associated timestamp(s), margin(s) of error for the coordinates (*i.e.*, “maps display radius”), and source(s) from which the location data was derived (*e.g.*, GPS, wi-fi, Bluetooth), if available. Google will not, in this step, provide the Google account identifiers (*e.g.*, example@gmail.com) associated with the devices or basic subscriber information for those accounts to the government.
- b. The government will identify to Google the devices appearing on the list produced in step 1 for which it seeks the Google account identifier and basic subscriber information. The government may, at its discretion, identify a subset of the devices.
- c. Google will then disclose to the government the Google account identifier associated with the devices identified by the government, along with basic subscriber information for those accounts.

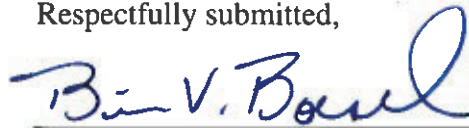
26. This process furthers efficiency and privacy by allowing for the possibility that the government, upon reviewing contextual information for all devices identified by Google, may be able to determine that one or more devices associated with a Google account (and the associated basic subscriber information) are likely to be of heightened evidentiary value and warrant further investigation before the records of other accounts in use in the area are disclosed to the government.

**CONCLUSION**

27. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c).

28. I further request that the Court direct Google to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



Brian V. Boesch  
Task Force Officer (TFO)  
Bureau of Alcohol, Tobacco, Firearms and  
Explosives (ATF)

October 28, 2022

Subscribed and sworn to before me on \_\_\_\_\_, 20\_\_\_\_

Kimberly A. Johnson  
United States Magistrate Judge



## **ATTACHMENT A**

### **Property To Be Searched**

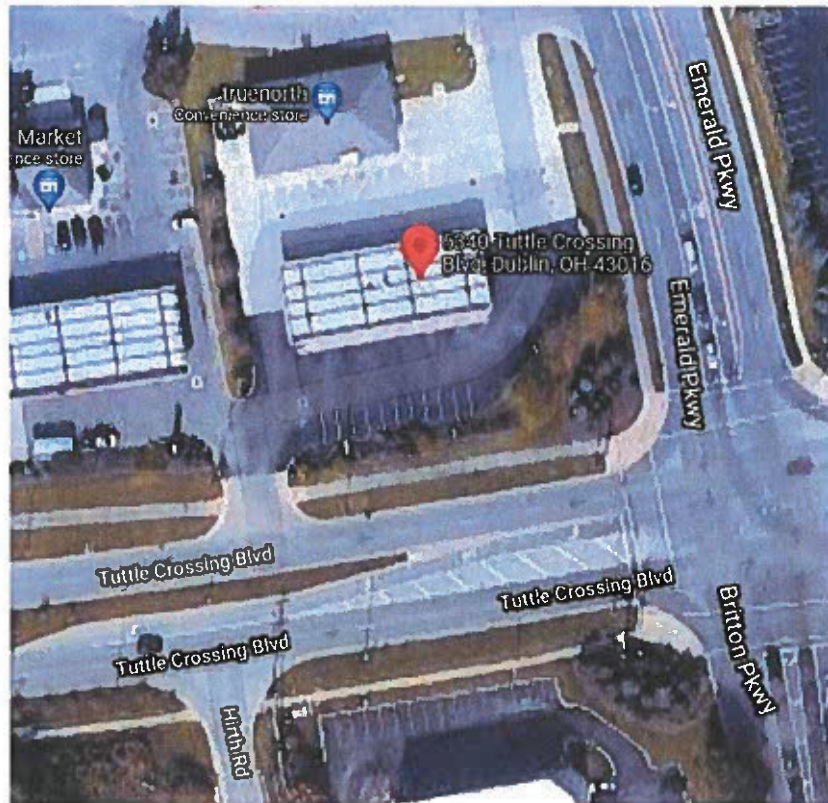
This warrant is directed to Google LLC and applies to:

- (1) Location History data, sourced from information including GPS data and information about visible wi-fi points and Bluetooth beacons transmitted from devices to Google, reflecting devices that Google calculated were or could have been (as indicated by margin of error, *i.e.*, “maps display radius”) located within the geographical region bounded by the latitudinal and longitudinal coordinates, dates, and times below (“Initial Search Parameters”); and
- (2) identifying information for Google Accounts associated with the responsive Location History data.

### **Initial Search Parameters**

#### **Search Parameter 1**

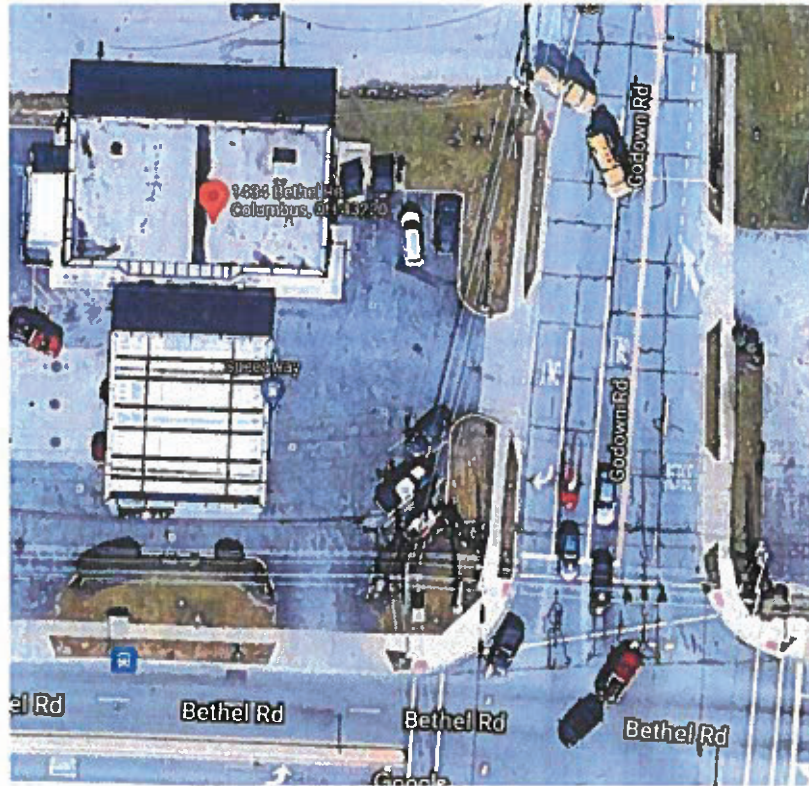
- Date: October 5, 2022
- Time Period (including time zone): 12:10am EST to 12:20am EST
- Target Location: Geographical area identified as
  - a polygon defined by at least three latitude/longitude coordinates in the format 40.075813, -83.141253 to 40.075872, -83.140577 to 40.075591, -83.140504 to 40.075494, -83.141206 connected by straight lines



#### Search Parameter 2

- Date: October 10, 2022
- Time Period (including time zone): 1:37am EST to 1:47am EST
- Target Location: Geographical area identified as
  - a polygon defined by at least three latitude/longitude coordinates in the format 40.064304, -83.057652 to 40.064321, -83.056832 to 40.063989, -83.056862 to 40.064033, -83.057675 connected by straight lines





### Search Parameter 3

- Date: October 22, 2022
- Time Period (including time zone): 11:12pm EST to 11:22pm EST
- Target Location: Geographical area identified as
  - a polygon defined by at least three latitude/longitude coordinates in the format 40.061901, -83.182222 to 40.061927, -83.181653 to 40.061567, -83.181588 to 40.061506, -83.182161 connected by straight lines





## **ATTACHMENT B**

### **Particular Items to Be Seized**

#### **I. Information to be disclosed by Google**

The information described in Attachment A, via the following process:

1. Google shall query location history data based on the Initial Search Parameters specified in Attachment A. For each location point recorded within the Initial SearchParameters, and for each location point recorded outside the Initial Search Parameters where the margin of error (*i.e.*, “maps display radius”) would permit the device to be located within the Initial Search Parameters, Google shall produce to the government information specifying the corresponding unique device ID, timestamp, location coordinates, display radius, and data source, if available (the “Device List”).
2. The government shall review the Device List and identify to Google the devices about which it seeks to obtain Google account identifier and basic subscriber information. The government may, at its discretion, identify a subset of the devices.
3. Google shall disclose to the government identifying information, as defined in 18 U.S.C. § 2703(c)(2), for the Google Accounts associated with each device ID appearing on the Device List about which the government inquires.

#### **II. Information to Be Seized**

All information described above in Section I that constitutes evidence of violations of 18 U.S.C. § 1951 and 18 U.S.C. § 924(c) have been committed on October 5, 10 and 22 of 2022, involving unknown person(s).